# Microsoft Azure MFA で SAML を利用した ASA AnyConnect VPN の設定

内容	
<u>はじめに</u>	
<u>前提条件</u>	
<u>要件</u>	
<u>使用するコンポーネント</u>	
<u>背景説明</u>	
SAMLコンポーネント	
署名および暗号化操作の証明書	
<u>ネットワーク図</u>	
<u>設定</u>	
<u> Microsoft App GalleryからのCisco AnyConnectの追加</u>	
<u>Azure ADユーザーのアプリへの割り当て</u>	
<u>CLIによるSAML用のASAの設定</u>	
<u>確認</u>	
<u>SAML認証を使用したAnyConnectのテスト</u>	
一般的な問題	
<u>エンティティIDの不一致</u>	
時間の不一致	
<u>誤ったIdP署名証明書の使用</u>	
<u>無効なアサーションオーディエンス</u>	
<u>アサーションコンシューマサービスのURLが正しくありません</u>	
SAML設定の変更が有効にならない	
トラブルシュート	
<u>関連情報</u>	
	_

# はじめに

このドキュメントでは、Adaptive Security Appliance(ASA)AnyConnectからMicrosoft Azure MFAを使用してSecurity Assertion Markup Language(SAML)を設定する方法について説明します 。

# 前提条件

## 要件

次の項目に関する知識があることが推奨されます。

- ASAでのRA VPN設定に関する基本的な知識。
- SAMLおよびMicrosoft Azureに関する基本的な知識
- AnyConnectライセンス対応(APEXまたはVPN-Only)

#### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Microsoft Azure ADサブスクリプション。
- ・ Cisco ASA 9.7+およびAnyconnect 4.6+
- AnyConnect VPNプロファイルの動作

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始していま す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認して ください。

## 背景説明

SAMLは、セキュリティドメイン間で認証および許可データを交換するためのXMLベースのフレ ームワークです。これにより、ユーザ、サービスプロバイダー(SP)、およびユーザが複数のサー ビスに対して一度にサインインできるアイデンティティプロバイダー(IdP)の間に信頼関係が構築 されます。Microsoft Azure MFAはCisco ASA VPNアプライアンスとシームレスに統合され、 Cisco AnyConnect VPNログインのセキュリティを強化します。

#### SAMLコンポーネント

メタデータ:IdPとSP間の安全なトランザクションを保証するXMLベースのドキュメントです。 IdPとSPが契約を交渉できる

デバイスでサポートされるロール(IdP、SP)

デバイスは複数のロールをサポートでき、SPとIdPの両方の値を含むことができます。 EntityDescriptorフィールドの下には、含まれている情報がシングルサインオンIdP用の場合は IDPSSODescriptorが、含まれている情報がシングルサインオンSP用の場合は SPSSODescriptorが表示されます。SAMLを正しく設定するには、適切なセクションから正しい 値を取得する必要があるため、これは重要です。

エンティティID:このフィールドは、SPまたはIdPの一意の識別子です。1つのデバイスに複数の サービスを設定し、異なるエンティティIDを使用してそれらを区別することができます。たとえ ば、認証が必要なトンネルグループごとにASAのエンティティIDが異なる場合などです。各トン ネルグループを認証するIdPには、これらのサービスを正確に識別するために、各トンネルグルー プに対して個別のエンティティIDエントリがあります。

ASAは複数のIdPをサポートでき、IdPごとに個別のエンティティIDを持って区別します。いずれ かの側が、以前に設定されたエンティティIDを含まないデバイスからメッセージを受信した場合 、デバイスはこのメッセージをドロップする可能性があり、SAML認証は失敗します。エンティ ティIDは、entityIDの横のEntityDescriptorフィールドに表示されます。

サービスURL:SPまたはIdPによって提供されるSAMLサービスへのURLを定義します。IdPsの場 合、これは最も一般的にはシングルログアウトサービスとシングルサインオンサービスです。 SPの場合、これは通常、アサーションコンシューマサービスとシングルログアウトサービスです。 。

IdPメタデータに含まれるSingle Sign-On Service URLは、SPが認証のためにユーザをIdPにリダ イレクトするために使用します。この値が正しく設定されていない場合、IdPはSPから送信され た認証要求を受信しないか、正常に処理できません。

SPメタデータで見つかったアサーションコンシューマサービスURLは、IdPによってユーザを SPにリダイレクトし、ユーザの認証の試行に関する情報を提供するために使用されます。この設 定が正しくない場合、SPはアサーション(応答)を受信しないか、正常に処理できません。

シングルログアウトサービスURLは、SPとIdPの両方にあります。これは、SPからのすべての SSOサービスのログアウトを容易にするために使用され、ASAではオプションです。IdPメタデ ータからのSLOサービスURLがSPで設定されている場合、ユーザーがSP上のサービスからログ アウトすると、SPはIdPに要求を送信します。IdPは、ユーザをサービスから正常にログアウトす ると、ユーザをSPにリダイレクトして戻し、SPのメタデータ内にあるSLOサービスURLを使用 します。

サービスURLのSAMLバインディング:バインディングは、SPが情報をIdPに転送したり、サービ スをIdPに転送したりするために使用する方法です。これには、HTTPリダイレクト、HTTP POST、アーティファクトが含まれます。データを転送する方法は、それぞれの方法で異なりま す。サービスによってサポートされるバインド方式は、そのサービスの定義内に含まれます。例 :SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location=<u>https://saml.example.com/simplesaml/saml2/idp/SSOService.php/</u> >ASAはアーティファ クトのバインドをサポートしていません。ASAはSAML認証要求に対して常にHTTPリダイレクト 方式を使用するため、HTTPリダイレクトバインディングを使用するSSOサービスURLを選択し て、IdPがこれを想定することが重要です。

#### 署名および暗号化操作の証明書

SPとIdPの間で送信されるメッセージの機密性と整合性を確保するために、SAMLにはデータを暗 号化して署名する機能が含まれています。データの暗号化や署名に使用される証明書をメタデー タに含めることで、受信側はSAMLメッセージを検証し、そのメッセージが予期されるソースか ら送信されていることを確認できます。署名と暗号化に使用される証明書は、KeyDescriptor use="signing"、KeyDescriptor use="encryption"の下のメタデータに含まれており、それぞれ X509Certificateの下にあります。ASAはSAMLメッセージの暗号化をサポートしていません。

# ネットワーク図



設定

# Microsoft App GalleryからのCisco AnyConnectの追加

ステップ1:Azure Portalにログインし、Azure Active Directoryを選択します。



ステップ2:次の図に示すように、Enterprise Applicationsを選択します。



ステップ3: ここで、次の図に示すようにNew Applicationを選択します。

Enterprise applications	All applications		
~	+ New application == Colum	nns	
Overview	🔗 Try out the new Enterprise Apps s	search preview! Click to enable the preview	$N. \rightarrow$
Overview     Diagnose and solve problems	Application Type	Applications status	Application visibility
olagnose and solve problems	Enterprise Applications $\checkmark$	Any 🗸	Any 🗸

ステップ 4:Add from the galleryセクションで、検索ボックスにAnyConnectと入力し、結果パネ ルからCisco AnyConnectを選択して、アプリケーションを追加します。

Add an application				Add app
				Cisco Systems, Inc.
Click here to try out the new	w and improved app gallery. $ ightarrow$			Empower your employees to work from anywhere, on compan
Application you're developing	On-premises application	Non-gallery application		laptops or personal mobile devices, at any time. AnyConnect simplifies secure endpoint access and provides the security necessary to help keep your organization safe and protected.
Register an app you're working on to integrate it with Azure AD	Application Proxy to enable secure remote access.	application that you don't find in the gallery		Use Microsoft Azure AD to enable user access to Cisco AnyConnect.
				Requires an existing Cisco AnyConnect subscription.
dd from the gallery Category All (3422)				Name O Cisco AnyConnect
AnyConnect		~	l	Publisher ① Cisco Systems, Inc.
1 applications matched "/	AnyConnect".			Single Sign-On Mode 🕕
Name		Category		SAML-based Sign-on
Cisco AnyConn	ect	Business management		URL ①
				https://www.ciscoanyconnect.com/
				Logo 🛈
				Add

ステップ 5 : 次の図に示すように、Single Sign-onメニュー項目を選択します。

AnyConnectVPN   Overvie	ew .		
«			
III Overview	Properties		
Deployment Plan	Name ①		
X Diagnose and solve problems	AnyConnectVPN		
Manage	Application ID 🕓		
Properties			
A Owners	Object ID 🛈		
Users and groups			
Single sign-on	Getting Started		
Provisioning			
Application proxy	1. Assign users and groups	2. Set up single sign on	3. Provision User Accounts
<ul> <li>Self-service</li> </ul>	Provide specific users and groups access to the applications	Enable users to sign into their application using their Azure AD credentials	Automatically create and delete user
Security	Assign users and groups	Get started	Get started
Seconditional Access			
Permissions			
Token encryption	4. Conditional Access	S. Self service	
Activity	Secure access to this application with a customizable access policy.	Enable users to request access to the application using their Azure AD	
Sign-ins	Create a policy	Get started	
🕍 Usage & insights (Preview)			

#### 手順6:図に示すように、SAMLを選択します。

#### Cisco AnyConnect | Single sign-on Select a single sign-on method Help me decide Overview Deployment Plan ¢ × Diagnose and solve problems Disabled SAML ତ Linked Link to an application in the Azure Active Directory Access Panel and/or User must manually enter their Rich and secure authentication to username and password. applications using the SAML (Security Manage Assertion Markup Language) protocol. Office 365 application launcher. Properties Owners Users and groups Single sign-on

#### 手順7:これらの詳細を使用してセクション1を編集します。

# <#root> a. Identifier (Entity ID) - https://<VPN URL>/saml/sp/metadata/<TUNNEL-GROUP NAME> b. Reply URL (Assertion Consumer Service URL) - https://<VPN URL>/+CSCOE+/saml/sp/acs?tgname=<TUNNEL-G Example: vpn url called asa.example.com and tunnel-group called AnyConnectVPN-1</pre>

Basic SAML Configuration		
Identifier (Entity ID)	Required	
Reply URL (Assertion Consumer Service URL)	Required	
Sign on URL	Optional	
Relay State	Optional	
Logout Url	Optional	

#### ステップ 8:SAML Signing Certificateセクションで、Downloadを選択して証明書ファイルをダウ ンロードし、コンピュータに保存します。

SAML Signing Certificate		Ú
Status	Active	
Thumbprint		
Expiration	5/1/2023, 4:04:04 PM	
Notification Email		
App Federation Metadata Url	https://l	
Certificate (Base64)	Download	
Certificate (Raw)	Download	
Federation Metadata XMI	Download	

#### ステップ9:これはASA設定に必要です。

- Azure AD Identifier これはVPN構成のsaml idpです。
- Login URL(ログインURL):これはURLサインインです。
- Logout URL:これはURLのサインアウトです。

Set up AnyConnectVPN You'll need to configure the application	on to link with Azure AD.	
Login URL	https://	
Azure AD Identifier	https://	
Logout URL	https://	

## Azure ADユーザーのアプリへの割り当て

このセクションでは、Cisco AnyConnectアプリへのアクセス権を付与する際に、Test1でAzureシ ングルサインオンの使用が有効になります。 ステップ1:アプリの概要ページで、Users and groups、Add userの順に選択します。

Cisco AnyConnect   l	Users and groups		
	Add user      Edit      Re     Re	move 🖉 Update Credentials   🗮 Columns   🛇 Got feedback?	
Overview	The application will appear on	the Access Panel for assigned users. Set 'visible to users?' to no in properties to prevent this	<i>→</i>
Deployment Plan			
🗙 Diagnose and solve problems	First 100 shown, to search all us	ers & groups, enter a display name.	
	Display Name	Object Type	Role assigned
Manage	No application assignments fou	ind	
Properties			
A Owners			
Users and groups			
Single sign on			

### ステップ2: Add AssignmentダイアログでUsers and groupsを選択します。

Add Assignment rchoga-azure-ad		,⊅ jsearch
Users and groups None Selected	>	
Select Role User	>	
		TE Test1

#### ステップ3: Add Assignmentダイアログで、Assignボタンをクリックします。

Select Role User	>
User	

CLIによるSAML用のASAの設定

ステップ1: トラストポイントを作成し、SAML証明書をインポートします。

config t

crypto ca trustpoint AzureAD-AC-SAML revocation-check none no id-usage

```
enrollment terminal
no ca-check
crypto ca authenticate AzureAD-AC-SAML
-----BEGIN CERTIFICATE-----
...
PEM Certificate Text you downloaded goes here
...
-----END CERTIFICATE-----
quit
```

#### ステップ2: これらのコマンドは、SAML IdPをプロビジョニングします。

webvpn

#### ステップ3: VPNトンネル設定へのSAML認証の適用

```
tunnel-group AnyConnectVPN-1 webvpn-attributes
  saml identity-provider https://xxx.windows.net/xxxxxxxxx/
  authentication saml
end
```

write memory

✤ 注:IdP設定を変更した場合、トンネルグループからsaml identity-provider設定を削除し、変更を有効にするために再適用する必要があります。

## 確認

#### SAML認証を使用したAnyConnectのテスト

ステップ1: VPN URLに接続し、Azure ADの詳細にログを入力します。

ステップ2:サインイン要求を承認します。





IPv4

00:00:22

# 一般的な問題

...

エンティティIDの不一致

デバッグ例:

[SAML] consume\_assertion:プロバイダーの識別子が不明#LassoServerす。#LassoServerオブ ジェクトにプロバイダを登録するには、lasso\_server\_add\_provider()または lasso\_server\_add\_provider\_from\_buffer()メソッドを使用する必要があります。

問題:通常、ASAのwebvpn設定でのsaml idp [entityID]コマンドが、IdPのメタデータで見つかったIdPエンティティIDと一致しないことを意味しています。

解決策:IdPのメタデータファイルのエンティティIDを確認し、これに一致するようにsaml idp [entity id]コマンドを変更します。

時間の不一致

デバッグ例:

[SAML] NotBefore:2017-09-05T23:59:01.896Z NotOnOrAfter:2017-09-06T00:59:01.896Zタイム アウト: 0

[SAML] consume\_assertion:アサーションが期限切れか、有効ではありません

問題 1. ASA時間がIdPの時間と同期されていません。

解決策 1.IdPで使用されるのと同じNTPサーバを使用してASAを設定します。

問題 2. 指定された時間の間はアサーションが無効です。

解決策 2. ASAで設定されているタイムアウト値を変更します。

#### 誤ったIdP署名証明書の使用

デバッグ例:

[Lasso] func=xmlSecOpenSSLEvpSignatureVerify:file=signatures.c:line=493:obj=rsasha1:subj=EVP\_VerifyFinal:error=18:data do not match:signature do not match ( データが一致し ない )

[SAML] consume\_assertion:プロファイルはメッセージの署名を確認できません

問題:ASAがIdPによって署名されたメッセージを確認できないか、確認するASAの署名がありま せん。

解決策:ASAにインストールされているIdP署名証明書を調べて、IdPによって送信される証明書と 一致することを確認します。これが確認されたら、シグニチャがSAML応答に含まれていること を確認します。

#### 無効なアサーションオーディエンス

デバッグ例:

[SAML] consume assertion:アサーションオーディエンスが無効です

問題:IdPは正しくない対象ユーザを定義しています。

解決方法: IdPの対象ユーザー構成を修正します。ASAのエンティティIDと一致している必要が あります。

アサーションコンシューマサービスのURLが正しくありません

デバッグの例:初期認証要求の送信後にデバッグを受信できない。ユーザはIdPでクレデンシャル を入力できますが、IdPはASAにリダイレクトしません。

問題:IdPが間違ったアサーションコンシューマサービスURLに対して設定されています。

解決方法:構成のベースURLを確認し、正しいことを確認してください。showを使用してASAメ タデータをチェックし、Assertion Consumer Service URLが正しいことを確認します。これをテ ストするには、参照します。ASAで両方とも正しい場合は、IdPをチェックしてURLが正しいこと を確認します。

SAML設定の変更が有効にならない

例:シングルサインオンURLが変更または変更された後も、SP証明書、SAMLはまだ機能せず、 以前の設定が送信されます。

問題:ASAに影響する設定変更があった場合、ASAはメタデータを再生成する必要があります。 これは自動的には行われません。

解決策:変更が行われた後、影響を受けるtunnel-groupでsaml idp [entity-id]コマンドを削除し、 再適用します。

# トラブルシュート

ほとんどのSAMLトラブルシューティングには、SAML構成のチェック時またはデバッグ実行時に 見つかる可能性のある構成の誤りが含まれています。debug webvpn saml 255は、ほとんどの問 題のトラブルシューティングに使用できますが、このデバッグで役に立つ情報が提供されないシ ナリオでは、追加のデバッグを実行できます。

# 関連情報

 アプリケーションプロキシを使用したオンプレミスアプリケーション用のSAMLシングルサ インオン 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人に よる翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっ ても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性につ いて法的責任を負いません。原典である英語版(リンクからアクセス可能)もあわせて参照する ことを推奨します。